

**CLAIMS**

**WHAT IS CLAIMED IS:**

1. A memory management unit for managing a memory storing data arranged within a plurality of memory pages, the memory management unit comprising:

5

a security check unit coupled to receive a physical address generated during execution of a current instruction, wherein the physical address resides within a selected memory page, and wherein the security check unit is configured to use the physical address to access at least one security attribute data structure located in the memory to obtain a security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the security attribute of the selected memory page, and to produce an output signal dependent upon a result of the comparison; and

10

11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000

15

wherein the memory management unit is configured to access the selected memory page dependent upon the output signal.

20

2. The memory management unit as recited in claim 1, wherein the at least one security attribute data structure comprises a security attribute table directory and at least one security attribute table.

25

3. The memory management unit as recited in claim 2, wherein the security attribute table directory comprises a plurality of entries, and where each entry of the security attribute table directory includes a present bit and a security attribute table base address field, and wherein the present bit indicates whether or not a security attribute table corresponding to the security

attribute table directory entry is present in the memory, and wherein the security attribute table base address field is reserved for a base address of the security attribute table corresponding to the security attribute table directory entry.

5 4. The memory management unit as recited in claim 2, wherein the at least one security attribute table comprises a plurality of entries, and where each entry of the security attribute table includes a security context identification (SCID) field, and wherein the SCID field includes a plurality of bit positions, and wherein the bit positions form a binary representation of an SCID value, and wherein the SCID value is an integer value greater than or equal to 0,  
10 and wherein the SCID value indicates a security context level of a corresponding memory page.

5 5. The memory management unit as recited in claim 1, wherein the security attribute of the selected memory page comprises a security context identification (SCID) value, and wherein  
15 the SCID value is an integer value greater than or equal to 0 and indicates a security context level of the selected memory page.

6. The memory management unit as recited in claim 1, wherein the security attribute of the current instruction comprises a security context identification (SCID) value, and wherein the  
20 SCID value is an integer value greater than or equal to 0 and indicates a security context level of a memory page containing the current instruction.

7. The memory management unit as recited in claim 1, wherein the security check logic is configured to obtain the security attribute of the current instruction from the at least one  
25 security attribute data structure.

8. The memory management unit as recited in claim 1, wherein the output signal is a fault signal.

5 9. The memory management unit as recited in claim 1, wherein the security check unit is configured to receive a set of security attributes of the selected memory page in addition to the security attribute of selected memory page, and to produce the output signal dependent upon: (i) the result of the comparison of the numerical value conveyed by the security attribute of the current instruction to the numerical value conveyed by the security attribute of selected memory page, and (ii) the set of security attributes of the selected memory page.

10. The memory management unit as recited in claim 9, wherein the set of security attributes of the selected memory page comprise a user/supervisor (U/S) bit and a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates only read accesses are allowed to the selected memory page, and wherein R/W=1 indicates that both read and write accesses are allowed to the selected memory page.

11. A central processing unit, comprising:

an execution unit operably coupled to a memory, wherein the execution unit is configured to fetch instructions from the memory and to execute the instructions; and

a memory management unit (MMU) operably coupled to the memory and configured to manage the memory, wherein the MMU is configurable to manage the memory such that the memory stores data arranged within a plurality of memory pages, and wherein the MMU comprises:

a security check unit coupled to receive a physical address generated by the execution unit during execution of a current instruction, wherein the physical address resides within a selected memory page, and wherein the security check unit is configured to use the physical address to access at least one security attribute data structure located in the memory to obtain a security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the security attribute of selected memory page, and to produce an output signal dependent upon a result of the comparison; and

wherein the MMU is configured to access the selected memory page dependent upon the output signal.

12. A computer system, comprising:

a memory for storing data, wherein the data includes instructions;

a central processing unit (CPU), comprising:

an execution unit operably coupled to the memory, wherein the execution unit is configured to fetch instructions from the memory and to execute the instructions; and

5

a memory management unit (MMU) operably coupled to the memory and configured to manage the memory, wherein the MMU is configurable to manage the memory such that the memory stores the data arranged within a plurality of memory pages, and wherein the MMU comprises:

10  
15

a security check unit coupled to receive a physical address generated by the execution unit during execution of a current instruction, wherein the physical address resides within a selected memory page, and wherein the security check unit is configured to use the physical address to access at least one security attribute data structure located in the memory to obtain a security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the security attribute of selected memory page, and to produce an output signal dependent upon a result of the comparison; and

20

wherein the MMU is configured to access the selected memory page dependent upon the output signal.

13. A memory management unit for managing a memory storing data arranged within a plurality of memory pages, the memory management unit comprising:

5 a paging unit coupled to the memory and to receive a linear address produced during execution of a current instruction, and configured to use the linear address to produce a physical address within a selected memory page, wherein the paging unit is configured to use the linear address to access at least one paged memory data structure located in the memory to obtain security attributes of the selected memory page, and wherein the paging unit is configured to produce a fault signal dependent upon the security attributes of the selected memory page, and wherein the paging unit comprises:

10 a security check unit coupled to receive the physical address, and wherein the security check unit is configured to use the physical address to access at least one security attribute data structure located in the memory to obtain an additional security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the additional security attribute of selected memory page, and to produce an output signal dependent upon a result of the comparison; and

20 wherein the memory management unit is configured to access the selected memory page dependent upon the output signal.

14. The memory management unit as recited in claim 13, wherein the at least one security attribute data structure comprises a security attribute table directory and at least one security attribute table.

5 15. The memory management unit as recited in claim 14, wherein the security attribute table directory comprises a plurality of entries, and where each entry of the security attribute table directory includes a present bit and a security attribute table base address field, and wherein the present bit indicates whether or not a security attribute table corresponding to the security attribute table directory entry is present in the memory, and wherein the security attribute  
10 table base address field is reserved for a base address of the security attribute table corresponding to the security attribute table directory entry.

16. The memory management unit as recited in claim 14, wherein the at least one security attribute table comprises a plurality of entries, and where each entry of the security attribute  
15 table includes a security context identification (SCID) field, and wherein the SCID field includes a plurality of bit positions, and wherein the bit positions form a binary representation of an SCID value, and wherein the SCID value is an integer value greater than or equal to 0, and wherein the SCID value indicates a security context level of a corresponding memory page.

20 17. The memory management unit as recited in claim 13, wherein the additional security attribute of the selected memory page comprises a security context identification (SCID) value, and wherein the SCID value is an integer value greater than or equal to 0 and indicates a security context level of the selected memory page.

25

18. The memory management unit as recited in claim 13, wherein the security attribute of the current instruction comprises a security context identification (SCID) value, and wherein the SCID value is an integer value greater than or equal to 0 and indicates a security context level of a memory page containing the current instruction.

5

19. The memory management unit as recited in claim 13, wherein the security check unit is coupled to receive a current privilege level (CPL) of a current task including the current instruction, and to produce the output signal dependent upon: (i) the result of the comparison of the numerical values conveyed by the security attribute of the current instruction and the security attribute of selected memory page, and (ii) the CPL of the current task including the current instruction.

10

20. The memory management unit as recited in claim 13, wherein the physical address within the selected memory page includes a base address and an offset, and wherein the paging unit is configured to obtain the base address from the at least one paged memory data structure.

15

21. The memory management unit as recited in claim 13, wherein the at least one paged memory data structure comprises a page directory and at least one page table as defined by the x86 processor architecture.

20

22. The memory management unit as recited in claim 13, wherein the security attributes of the selected memory page comprise a user/supervisor (U/S) bit and a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the

25



operating system, and wherein  $U/S=1$  indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein  $R/W=0$  indicates only read accesses are allowed to the selected memory page, and wherein  $R/W=1$  indicates that both read and write accesses are allowed to the selected memory page.

5

23. A memory management unit for managing a memory storing data arranged within a plurality of memory pages, the memory management unit comprising:

a paging unit coupled to the memory and to receive a linear address produced during execution of a current instruction residing within a first memory page, wherein the paging unit is configured to use the linear address to produce a physical address accessed by the current instruction, and wherein the physical address includes a base address of a selected memory page and an offset, and wherein the paging unit is configured to access at least one paged memory data structure located in the memory using the linear address to obtain the base address and security attributes of the selected memory page, and wherein the paging unit is configured to receive a security attribute of the instruction, and wherein the paging unit is configured to produce a fault signal dependent upon the security attribute of the instruction and the security attributes of the selected memory page, and wherein the paging unit comprises:

a security check unit coupled to receive the security attribute of the instruction, the security attributes of the selected memory page, and the physical address within the selected memory page, and wherein the security check unit is configured to use the physical address to access

25

at least one security attribute data structure located in the memory to obtain an additional security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the additional security attribute of selected memory page, and to produce an output signal dependent upon a result of the comparison; and

wherein the memory management unit is configured to access the selected memory page dependent upon the output signal.

24. The memory management unit as recited in claim 23, wherein the at least one paged memory data structure comprises a page directory and at least one page table as defined by the x86 processor architecture.

25. The memory management unit as recited in claim 23, wherein the security attribute of the current instruction comprises a current privilege level (CPL) of a task including the current instruction as defined by the x86 processor architecture.

26. The memory management unit as recited in claim 23, wherein the security attributes of the selected memory page comprise a user/supervisor (U/S) bit a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates

only read accesses are allowed to the selected memory page, and wherein R/W=1 indicates that both read and write accesses are allowed to the selected memory page.

27. The memory management unit as recited in claim 23, wherein the additional security  
5 attribute of the selected memory page comprises a security context identification (SCID) value, and wherein the SCID value is an integer value greater than or equal to 0 and indicates a security context level of the selected memory page.

28. The memory management unit as recited in claim 23, wherein the security attribute of  
10 the current instruction comprises a security context identification (SCID) value, and wherein the SCID value is an integer value greater than or equal to 0 and indicates a security context level of the first memory page containing the current instruction.

29. The memory management unit as recited in claim 23, wherein the at least one security  
15 attribute data structure comprises a security attribute table directory and at least one security attribute table.

30. The memory management unit as recited in claim 29, wherein the security attribute table  
20 directory comprises a plurality of entries, and where each entry of the security attribute table directory includes a present bit and a security attribute table base address field, and wherein the present bit indicates whether or not a security attribute table corresponding to the security attribute table directory entry is present in the memory, and wherein the security attribute table base address field is reserved for a base address of the security attribute table corresponding to the security attribute table directory entry.

31. The memory management unit as recited in claim 29, wherein the at least one security attribute table comprises a plurality of entries, and where each entry of the security attribute table includes security context identification (SCID) field, and wherein the SCID field includes a plurality of bit positions, and wherein the bit positions form a binary representation of an SCID value, and wherein the SCID value is an integer value greater than or equal to 0, and wherein the SCID value indicates a security context level of a corresponding memory page.

32. A method for providing access security for a memory used to store data arranged within a plurality of memory pages, the method comprising:

receiving a linear address produced during execution of an instruction and a security attribute of the instruction, wherein the instruction resides in a first memory page;

using the linear address to access at least one paged memory data structure located in the memory to obtain a base address of a selected memory page and security attributes of the selected memory page;

combining the base address of the selected memory page with an offset to produce a physical address within the selected memory page if the security attribute of the instruction and the security attributes of the selected memory page indicate the access is authorized;

generating a fault signal if the security attribute of the instruction and the security attributes of the selected memory page indicate the access is not authorized;

accessing at least one security attribute data structure located in the memory using the physical address of the selected memory page to obtain an additional security attribute of the first memory page and an additional security attribute of the selected memory page;

comparing a numerical value conveyed by an additional security attribute of the first memory page to a numerical value conveyed by the additional security attribute of selected memory page; and

accessing the selected memory page dependent upon a result of the comparing of the numerical values conveyed by the security attribute of the first memory page and the additional security attribute of selected memory page.

33. The method as recited in claim 32, wherein the receiving comprises:

receiving a linear address produced during execution of an instruction and a security attribute of the instruction, wherein the instruction resides in a first memory page, and wherein the security attribute of the instruction comprises a current privilege level (CPL) of a task including the instruction as defined by the x86 processor architecture.

34. The method as recited in claim 32, wherein the using comprises:

using the linear address to access at least one paged memory data structure located in the memory to obtain a base address of a selected memory page and security attributes of the selected memory page, wherein the at least one paged memory data structure comprises a page directory and at least one page table as defined by the x86 processor architecture.

35. The method as recited in claim 31, wherein the combining comprises:

combining the base address of the selected memory page with an offset to produce a physical address within the selected memory page if the security attribute of the instruction and the security attributes of the selected memory page indicate the access is authorized, wherein the security attributes of the selected memory page comprise a user/supervisor (U/S) bit a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates only read accesses are allowed to the selected memory page, and wherein R/W=1 indicates that both read and write accesses are allowed to the selected memory page.

36. The method as recited in claim 31, wherein the generating comprises:

generating a fault signal if the security attribute of the instruction and the security attributes of the selected memory page indicate the access is not authorized, wherein the fault signal is a general protection fault (GPF) signal as defined by the x86 processor architecture.

5

37. The method as recited in claim 31, wherein the accessing comprises:

accessing at least one security attribute data structure located in the memory using the physical address of the selected memory page to obtain an additional security attribute of the first memory page and an additional security attribute of the selected memory page, wherein the at least one security attribute data structure comprises a security attribute table directory and at least one security attribute table, and wherein the additional security attribute of the first memory page comprises a security context identification (SCID) value of the first memory page, and wherein the SCID value of the first memory page is an integer value greater than or equal to 0 and indicates a security context level of the first memory page, and wherein the additional security attribute of the selected memory page comprises a security context identification (SCID) value of the selected memory page, and wherein the SCID value of the selected memory page is an integer value greater than or equal to 0 and indicates a security context level of the selected memory page.

10

15

20